CLAIMS:

1. Device for authorizing a user to get access to content stored in encrypted form on a storage medium (10), said storage medium storing a machine-readable medium identifier (id) and at least one key table (KL) encrypted by use of a key table key (KLK) and storing at least one asset key (AK) for decrypting encrypted content (C), said device comprising:

- a connection means (6) for connecting said device to a network (3),
- a drive (5) for accessing said storage medium (10), in particular for reading content (C) and said medium identifier (id) from said storage medium (10), and
- a transmitter (7) for transmitting said medium identifier (id) and a user identifier (ui) of a user, who shall be authorized to get access to said content (C) and who is identified to said network (3) by said user identifier (ui), to an authentication unit (AuC) within said network (3), said medium identifier (id) and said user identifier (ui) being used by said authentication unit (AuC) for generating a key table key (KLK) for said user enabling said user to decrypt at least one predetermined key table (KL).

2. Device as claimed in claim 1,
further comprising a receiver (8) for receiving said key table key (KLK) for said user from said network (3), and
wherein said transmitter (7) is operative for transmitting said received key table key (KLK) to said user.

3. Device as claimed in claim 1,
wherein said storage medium (10) stores a plurality of key tables (KL), in particular one key table per user, wherein to each key table (KL) a user check identifier (uc) is assigned and
wherein said device further comprises a user check means (11) for checking based on said user check identifier (uc) which key table (KL) is assigned to said user.

4. Device as claimed in claim 1,

wherein said at least one key table (KL) further comprises a decryption check identifier (DC) and wherein said device further comprises a decryption check means (9) for checking based on said decryption check identifier (DC) if a key table (KL) has been correctly decrypted.

5. Device as claimed in claim 1,
further comprising a key table generating means (12) for generating a key table (KL) by encryption of one or more asset keys (AK) by use of a key table key (KLK), and
wherein said drive (5) is operative for storing said key table (KL) on said storage medium (10).

6. Device as claimed in claim 1,
wherein said device is a mobile communication device, in particular a mobile phone, wherein said network is a mobile communication network and wherein said authentication unit (AuC) uses an authentication algorithm used for authentication of mobile communication devices for generating said key table key (KLK).

7. Device as claimed in claim 6,
wherein said user identifier (ui) is the international mobile subscriber identity or the telephone number of said user.

8. Device as claimed in claim 6,
wherein said transmitter (7) is operative for transmitting said medium identifier (id) and said user identifier (ui) to an authentication unit (AuC) of the home location register of said user with said network (3).

9. Method of authorizing a user to get access to content stored in encrypted form on a storage medium (10), said storage medium storing a machine-readable medium identifier (id) and at least one key table (KL) encrypted by use of a key table key (KLK) and storing at least one asset key (AK) for decrypting encrypted content (C), said method comprising the steps of:

- connecting said device to a network (3), and
- transmitting said medium identifier (id) and a user identifier (ui) of a user,

who shall be authorized to get access to said content (C) and who is identified to said network (3) by said user identifier (ui), to an authentication unit (AuC) within said network

(3), said medium identifier (id) and said user identifier (ui) being used by said authentication unit (AuC) for generating a key table key (KLK) for said user enabling said user to decrypt at least one predetermined key table (KL).

10. Network comprising:

- a first user device (1) for authorizing a user of a second user device to get access to content stored in encrypted form on a storage medium (10), said storage medium storing a machine-readable medium identifier (id) and at least one key table (KL) encrypted by use of a key table key (KLK) and storing at least one asset key (AK) for decrypting encrypted content (C), said first user device comprising:

- a connection means (6) for connecting said device to a network (3),

- a drive (5) for accessing said storage medium (10), in particular for reading content (C) and said medium identifier (id) from said storage medium (10), and

- a transmitter (7) for transmitting said medium identifier (id) and a user identifier (ui) of a user, who shall be authorized to get access to said content (C) and who is identified to said network (3) by said user identifier (ui), to an authentication unit (AuC) within said network (3);

- an authentication unit (AuC) comprising:

- a receiver (30) for receiving said medium identifier (id) and said user identifier (ui),

- a key generating means (31) for generating a key table key for said user using said medium identifier (id) and said user identifier (ui), said key table key enabling said user to decrypt said at least one key table, and

- a transmitter (32) for transmitting said key table key to said first and/or said second user device; and

- a second user device (2) of a user who shall be authorized to get access to content stored in encrypted form on said storage medium comprising:

- a connection means (6) for connecting said device to said network,

- a receiver (8) for receiving said key table key from said authentication unit or said first user device,

- a drive (5) for accessing said storage medium, in particular for reading content from said storage medium, and for decrypting at least one predetermined key table using the received key table key.

11. Computer program comprising program code means for causing a computer to carry out the steps of the method as claimed in claim 9 when said computer program is run on a computer.